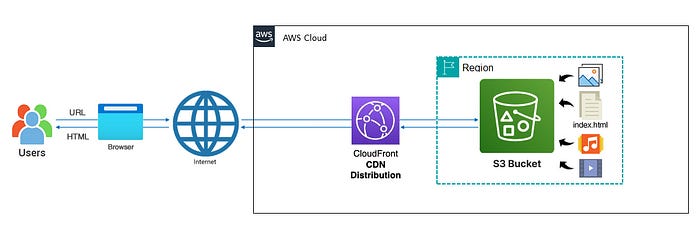
**Hosting my Static Website in an AWS S3 Bucket + CloudFront— Part 2**

**Serving end-users with Amazon CloudFront**

[[](https://medium.com/@rogernem?source=post_page-----3b71e3375a1f--------------------------------) Roger Nem](https://medium.com/@rogernem?source=post_page-----3b71e3375a1f--------------------------------) 6 min read Jan 4, 2024



— Architecture Diagram of Hosting my Professional Resume Website in an AWS S3 Bucket + CloudFront (picture by author)

In my introductory “[**Hosting my Static Website in an AWS S3 Bucket — Part 1**](https://medium.com/@rogernem/hosting-my-static-website-in-an-aws-s3-bucket-d5e1d94417f4)” article of a series dedicated to guide you on how to host a static website in an AWS S3 Bucket, I showed the step-by-step to do exactly that.

By now you should have an AWS S3 website Bucket created and all of your website content there.

As an improvement of my initial solution, in this part 2 of the series we will use Amazon CloudFront to securely deliver our static website content with low latency and high transfer speeds to our end-users.

# Table of Contents

1. [Content Delivery Network (CDN)](https://medium.com/@rogernem/hosting-my-static-website-in-an-aws-s3-bucket-cloudfront-part-2-3b71e3375a1f#9d24)
2. [Amazon CloudFront](https://medium.com/@rogernem/hosting-my-static-website-in-an-aws-s3-bucket-cloudfront-part-2-3b71e3375a1f#934e)
3. [Creating the CloudFront Distribution](https://medium.com/@rogernem/hosting-my-static-website-in-an-aws-s3-bucket-cloudfront-part-2-3b71e3375a1f#ba99)
4. [Securing the Origin (Bonus)](https://medium.com/@rogernem/hosting-my-static-website-in-an-aws-s3-bucket-cloudfront-part-2-3b71e3375a1f#f58d)

# Content Delivery Network (CDN)

A Content Delivery Network (CDN) is a distributed network of servers strategically positioned across various geographical locations to efficiently deliver web content, such as images, videos, stylesheets, scripts, and other assets, to end-users. The primary goal of a CDN is to enhance the performance, reliability, and availability of web content by reducing latency and optimizing the delivery process.

**Benefits of Using a CDN:**

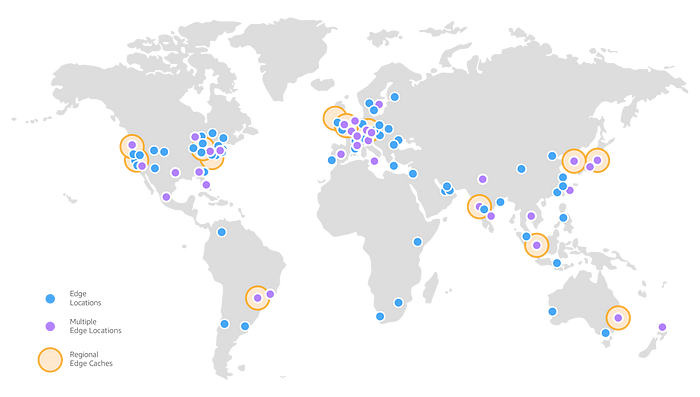
1. **Improved Website Performance:** CDNs cache content on multiple servers, allowing users to access data from a server geographically closer to them. This reduces latency and accelerates the loading time of web pages.
2. **Global Reach and Scalability:** CDNs consist of a network of servers distributed worldwide. This global presence ensures that content is delivered quickly to users regardless of their location, enhancing the scalability and reach of websites or applications.
3. **Bandwidth Savings:** CDNs reduce the load on the origin server by distributing content delivery across multiple servers. This helps in minimizing the overall bandwidth usage, leading to cost savings for website owners.
4. **Load Balancing:** CDNs employ load balancing mechanisms to distribute incoming traffic across multiple servers. This ensures that no single server becomes overloaded, improving overall performance and reliability.
5. **Enhanced Security:** CDNs provide security features such as DDoS protection, SSL/TLS encryption, and web application firewall (WAF) services. These features help safeguard websites from various online threats.
6. **Increased Reliability and Redundancy:** With content replicated on multiple servers, CDNs offer redundancy. If one server fails, traffic is automatically routed to another, ensuring continuous content delivery even in the event of server failures.
7. **Faster Content Delivery for Mobile Users:** CDNs optimize content delivery for mobile devices, reducing load times and improving the user experience for visitors accessing websites from smartphones and tablets.
8. **SEO Benefits:** Faster page load times, which CDNs contribute to, are a positive factor in search engine rankings. This can lead to improved visibility and ranking on search engine results pages.
9. **On-Demand Scalability:** CDNs provide on-demand scalability to handle traffic spikes or increased demand for specific content. This is particularly valuable for websites experiencing sudden popularity or events.
10. **Analytics and Reporting:** CDNs often include analytics and reporting tools, allowing website owners to gain insights into user behavior, traffic patterns, and performance metrics.

By leveraging these benefits, CDNs play a crucial role in optimizing the delivery of web content, ensuring a faster, more reliable, and secure online experience for users globally.

# Amazon CloudFront

[AWS CloudFront](https://aws.amazon.com/cloudfront/) (CF) is the AWS fast, programmable and secure Content Delivery Network (CDN) and it is a Global (not Regional) service, consisting of a network of Edge Locations distributed across the globe.

To deliver content to end users with lower latency, Amazon CloudFront uses a global network of 600+ Points of Presence and 13 regional edge caches in 100+ cities across 50 countries. (As of January 2024 — Source: [AWS Documentation](https://aws.amazon.com/cloudfront/features/?whats-new-cloudfront.sort-by=item.additionalFields.postDateTime&whats-new-cloudfront.sort-order=desc)).



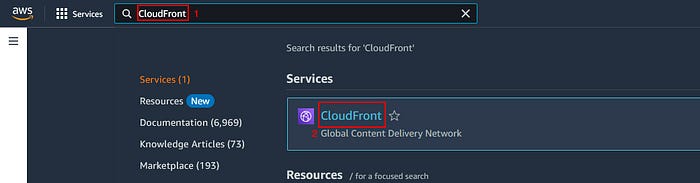
As of January 2024 — AWS Edge Locations | Source: AWS Documentation

When a user requests content that you’re serving with CloudFront, the request is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

* If the content is already in the edge location with the lowest latency, CloudFront delivers it immediately.
* If the content is not in that edge location, CloudFront retrieves it from an origin that you’ve defined — the Amazon S3 website bucket in our case.

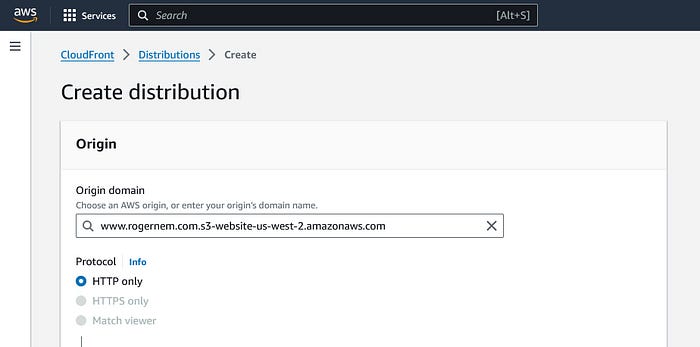
# Creating the CloudFront Distribution

1. Sign in to the AWS Management Console.
2. Search for “**CloudFront**” (1) and click on “**CloudFront**” (2) under Services.



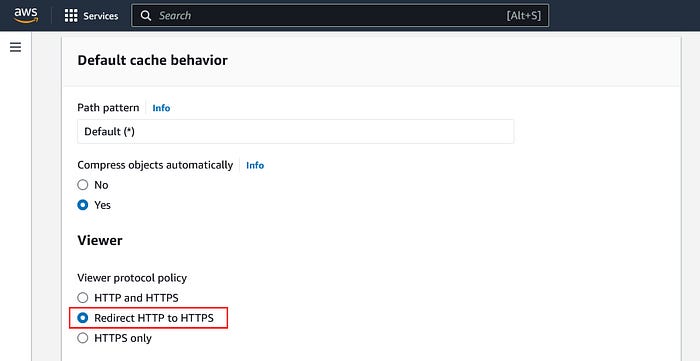
(picture by author)

3. Click on “**Create a CloudFront Distribution**” button.  
4. Paste your AWS S3 Bucket URL under “Origin domain”.  
(e.g. [www.rogernem.com.s3-website-us-west-2.amazonaws.com](http://www.rogernem.com.s3-website-us-west-2.amazonaws.com))



(picture by author)

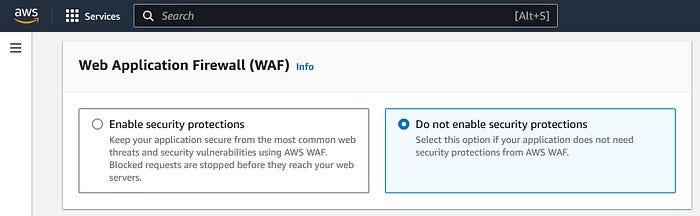
5. **Scroll down** to the “**Default cache behavior”** section and under “**Viewer protocol policy”**, select “**Redirect HTTP to HTTPS”**.



(picture by author)

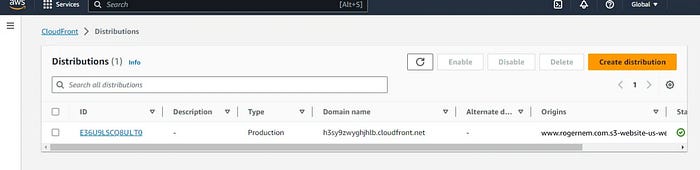
6. Under “**Web Application Firewall (WAF)**”, click on “**Do not enable security protections**”.

Note: To protect your web applications from common exploits this should be enabled. Please refer to <https://aws.amazon.com/waf/> for more information.



(picture by author)

7. Leave everything else as **default** and click on “**Create distribution**”.

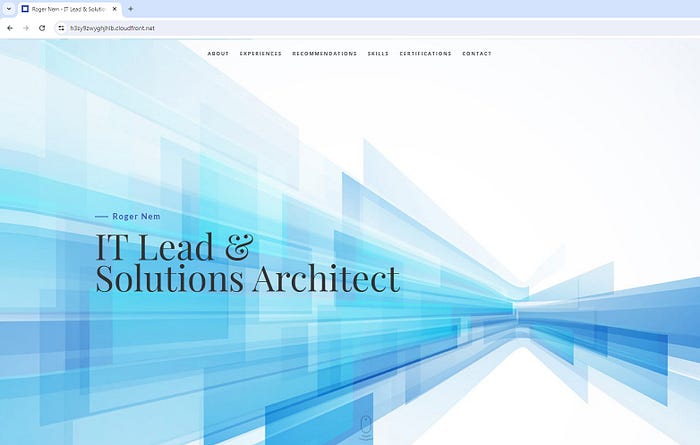


(picture by author)

8. **Click** on your **Distribution ID   
9.** Under the “**General”** tab **click** to copy the **“Distribution domain name”** link: <https://h3sy9zwyghjhlb.cloudfront.net/>

10. Open a new tab in your Browser, paste the URL and hit enter.

You should be able to see your website now using the Distribution domain name instead. Yay!🎉 Congratulations.



— www.rogernem.com (picture by author)

# Securing the Origin (Bonus)

CloudFront Edge locations are strategically positioned between the origin and the end-user, forming a dynamic architecture that enables users to access both the origin and CloudFront (CF) edge locations through public URLs. However, it is essential to note that this approach raises security concerns and falls short of best practices. The exposure of both the origin and CF edge locations to users via public URLs poses potential vulnerabilities, necessitating a more secure and prudent approach to ensure robust data protection and adherence to industry standards.

Therefore, CloudFront can implement multiple ways to prevent this.

1. Restricting S3 origins
2. Restricting custom origins using custom headers
3. Restricting custom origins using firewalls
4. Geo-restrictions

We will use the first option to restrict origins using OAC.

## 1.0 Restricting S3 Access with Origin Access Control (OAC)

CloudFront provides two ways to send authenticated requests to an Amazon S3 origin: origin access control (OAC) and origin access identity (OAI). It is recommended to use OAC because it supports:

* All Amazon S3 buckets in all AWS Regions, including opt-in Regions launched after December 2022
* Amazon S3 [server-side encryption with AWS KMS](https://docs.aws.amazon.com/AmazonS3/latest/userguide/serv-side-encryption.html) (SSE-KMS)
* Dynamic requests (PUT and DELETE) to Amazon S3

Origin access identity (OAI) doesn’t work for the scenarios in the preceding list, or it requires extra workarounds in those scenarios.

Please refer to <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html> to do this.

**If you enjoyed this article and found it helpful, please don’t forget to leave a heart** ❤**, comment** 💬**, clap** 👏🏻**, and share** ➦ **it to show your support.**

**Also, don’t forget to** [**connect**](https://www.linkedin.com/in/rogertn/)**,** [**follow me**](https://medium.com/@rogernem) **for more articles and support me by** [buying me a coffee](https://buymeacoffee.com/rogernem)**.** :-) **Thank you!**

References:  
- <https://en.wikipedia.org/wiki/Content_delivery_network>  
- <https://aws.amazon.com/cloudfront/>  
- <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>  
- <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>  
- <https://aws.amazon.com/waf/>

[Aws In Plain English](https://medium.com/tag/aws-in-plain-english?source=post_page-----3b71e3375a1f---------------aws_in_plain_english-----------------)

[Cdn](https://medium.com/tag/cdn?source=post_page-----3b71e3375a1f---------------cdn-----------------)

[Cloudfront](https://medium.com/tag/cloudfront?source=post_page-----3b71e3375a1f---------------cloudfront-----------------)

[S3](https://medium.com/tag/s3?source=post_page-----3b71e3375a1f---------------s3-----------------)

[Security](https://medium.com/tag/security?source=post_page-----3b71e3375a1f---------------security-----------------)